

Forget it (Solution)

Ini adalah soal Memory Forensics. Solusi dibangun dengan Volatility (<https://github.com/volatilityfoundation/volatility>). Namun dengan cara naif seperti membuka file di Notepad atau Hex Editor juga dapat menjadi solusi namun flag dibuat dengan sedikit obfuscation sehingga pencarian "ara2021" pada file tidak akan mengeluarkan apa-apa. Walaupun begitu, terdapat beberapa cara yang jauh lebih rumit dan unintended seperti regex namun akan menghabiskan waktu lebih lama daripada solusi yang diniatkan.

Langkah-langkah solusinya adalah sebagai berikut:

1. Mengenali memory dump
2. Menentukan process of interest
3. Menggali informasi mengenai process tersebut
4. Mengekstrak file berdasarkan process yang menarik
5. Mendapatkan flagnya

Mengenali memory dump

Hal pertama yang dilakukan adalah mengenali OS dari memory dump ini. Volatility memiliki modul untuk mengenali OS dengan command line berikut:

```
python vol.py -f <lokasi file> imageinfo
```

```
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x8273fde8L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x80b96000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2021-01-18 09:20:27 UTC+0000
      Image local date and time : 2021-01-18 01:20:27 -0800
```

Volatility akan mengenalinya sebagai Windows 7 SP1 32-bit. Setelah ini OS ini akan berguna untuk volatility agar dapat memproses process.

Menentukan process of interest

Setelah mengenali OS, lakukan identifikasi proses yang sedang berjalan dengan command line berikut:

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 cmdline
```

```

Command line :
*****
cygrunsrv.exe pid: 2004
*****
conhost.exe pid: 2036
Command line :
*****
sshd.exe pid: 312
Command line :
*****
wLms.exe pid: 348
Command line : C:\Windows\system32\wLms\wLms.exe
*****
sppsvc.exe pid: 1684
Command line : C:\Windows\system32\sppsvc.exe
*****
StikyNot.exe pid: 1968
Command line : "C:\Windows\System32\StikyNot.exe"
*****
VSSVC.exe pid: 2116
Command line : C:\Windows\system32\vssvc.exe
*****
svchost.exe pid: 2204
Command line : C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
*****
SearchIndexer.exe pid: 2268
Command line : C:\Windows\system32\SearchIndexer.exe /Embedding
*****
svchost.exe pid: 2976
Command line : C:\Windows\System32\svchost.exe -k secsvcs
*****
wuauclt.exe pid: 3444
Command line :
*****
calc.exe pid: 3612
Command line : "C:\Windows\system32\calc.exe"
*****
notepad.exe pid: 3800
Command line : "C:\Windows\system32\notepad.exe"
*****
svchost.exe pid: 2424
Command line : C:\Windows\System32\svchost.exe -k swprv
*****
wordpad.exe pid: 2768
Command line : "C:\Program Files\Windows NT\Accessories\wordpad.exe"
*****
DumpIt.exe pid: 4032
Command line : "C:\Users\IEUser\Downloads\DumpIt.exe"
*****
conhost.exe pid: 4080
Command line : \??\C:\Windows\system32\conhost.exe "2067260208-5384559521251032766-2098284282-13999195251920462557148425781974235785

```

Umumnya proses yang berada di atas adalah proses sistem, sedangkan proses di daerah bawah adalah proses yang dimulai oleh user.

Terdapat beberapa aplikasi yang dijalankan oleh user, yang menarik adalah Sticky Note, Calculator, Notepad, dan Wordpad.

Dalam soal ini, proses yang mengarah menuju solusi adalah **Sticky Note**. Petunjuk yang diberikan di soal adalah **pelupa**. Seorang pelupa yang berada di lingkungan kerja umumnya menggunakan pengingat, dan mengarahkan peserta ke reminder, dalam hal ini Sticky Note.

Menggali informasi mengenai process tersebut

Sticky Note menyimpan data yang tertulis pada masing-masing notes tersebut pada sebuah file. Pada Windows 7, file ini berada di **C:\Users\<nama user>\AppData\Roaming\Microsoft\Sticky Notes*.snt**

File .snt terisi mirip seperti Word, di mana data diappend berdasarkan pengetikan terakhir.

Kemudian gunakan module filescan untuk melakukan mapping file yang dicache pada memory.

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 filescan > output.txt
```

Offset (P)	#Ptr	#Ind	Access	Name
0x000000000002e790	3	0	R--rwd	Device\HarddiskVolume1\Windows\System32\werapi.dll
0x0000000000062768	3	0	RW----	Device\HarddiskVolume1\Directory
0x00000000001b69568	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\sscore.dll
0x00000000001b69d90	8	0	RW----	Device\HarddiskVolume1\ProgramData\Microsoft\RAC\StateData\RacWinDataBookmarks.dat
0x00000000001ddaf80	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\batmeter.dll
0x00000000002227038	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\dsmsgapi.dll
0x00000000002404b0	8	0	W-----	Device\HarddiskVolume1\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_6.1.7601_e292ae971bf3d8d72d7a0f2730de3d1dab8dce_039d3db2\Report.wer
0x0000000000252fbc0	8	0	R--rd	Device\HarddiskVolume1\Windows\Fonts\smallf.fon
0x000000000030d8498	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\nci.dll
0x000000000030d8490	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\logoncli.dll
0x000000000036cae60	5	0	R--rd	Device\HarddiskVolume1\Windows\Fonts\verdana.ttf
0x000000000037c4248	8	0	R--rd	Device\HarddiskVolume1\Windows\System32\wshgss.dll
0x000000000047f54c0	7	0	R--rd	Device\HarddiskVolume1\Windows\System32\wscvcs.dll
0x000000000047f6f50	7	0	R--rd	Device\HarddiskVolume1\Program Files\Windows Defender\MpSvc.dll
0x000000000047f7038	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\WSOapi.dll
0x000000000047f7a28	8	1	R--rd	Device\HarddiskVolume1\ProgramData\Microsoft\Windows Defender\Scans\mpcache-6CCA129E8FC7EF1A523765643C275A9A43C652B.bin.79
0x000000000047f8560	3	1	RW-r--	Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender\40Operational.evtx
0x000000000047f9ac0	3	0	RW-rwd	Device\HarddiskVolume1\Directory
0x000000000047f93e0	1	1	R--rd	Device\HarddiskVolume1\Windows\System32\en-US\crypt32.dll.mui
0x000000000047fc290	3	0	R--rd	Device\HarddiskVolume1\Windows\System32\wsapi.dll
0x000000000047fc7d8	3	1	RW-r--	Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkAccessProtection\4WHC.evtx
0x000000000047fdee8	1	0	R--rd	Device\HarddiskVolume1\Windows\explorer.exe
0x000000000048fb688	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\powertracker.dll
0x00000000004a4af0	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\api-ms-win-downlevel-normaliz-l1-l-0-0.dll
0x00000000004c38a08	3	0	R--rd	Device\HarddiskVolume1\Windows\System32\rasadhlp.dll
0x00000000004f65530	11	0	RW-rwd	Device\HarddiskVolume1\Directory
0x00000000004f9a370	3	0	R--rd	Device\HarddiskVolume1\Windows\System32\winhttp.dll
0x00000000004f9ac00	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\winhtr.dll
0x00000000005c124b8	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\wbem\esscli.dll
0x00000000007a782c0	8	0	RW-rw-	Device\HarddiskVolume1\ProgramData\Microsoft\RAC\PublishedData\RacWinDatabase.sdf
0x00000000008b9ec8	1	1	R--rd	Device\HarddiskVolume1\Windows\Fonts\StaticCache.dat
0x00000000008d84270	11	0	RW-rwd	Device\HarddiskVolume1\Directory
0x000000000096a2768	3	0	RW-rwd	Device\HarddiskVolume1\Directory
0x0000000000a13ca40	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\ysentyfy.dll
0x0000000000a08ca58	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\ncobjapi.dll
0x0000000000af9d458	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\taskcomp.dll
0x0000000000bd0d6f0	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\sgmapi.dll
0x0000000000de4e68	5	0	R--rd	Device\HarddiskVolume1\Windows\System32\sscore.dll
0x0000000000deee50	3	0	RW-rwd	Device\HarddiskVolume1\Directory
0x0000000001f69038	5	0	R--rd	Device\HarddiskVolume1\Windows\Fonts\georgia.ttf
0x0000000001f09550	9	1	R--rd	Device\HarddiskVolume1\Windows\System32\en-US\odbcint.dll.mui

Kemudian cari file .snt untuk Sticky Note.

0x000000007ec87798	17	0	RW-rwd	Device\HarddiskVolume1\Directory
0x000000007ec87d58	1	1	R--rd	Device\HarddiskVolume1\Windows\System32\en-US\setupapi.dll.mui
0x000000007ec88038	5	0	R--rd	Device\HarddiskVolume1\Windows\System32\ActionCenter.dll
0x000000007ec886b0	1	1	R--rd	Device\HarddiskVolume1\Windows\System32\en-US\KernelBase.dll.mui
0x000000007ec88ce0	8	1	RW-r--	Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
0x000000007ec896c0	3	0	R--rd	Device\HarddiskVolume1\Windows\System32\FwRemoteSvr.dll
0x000000007ec8a2b0	1	1	R--rw-	Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.
0x000000007ec8a470	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\WwanAPI.dll
0x000000007ec8a848	4	0	R--rd	Device\HarddiskVolume1\Windows\System32\diagperf.dll
0x000000007ec8ab30	1	0	R--rd	Device\HarddiskVolume1\Windows\System32\wscinterop.dll
0x000000007ec8c290	2	1	R--rd	Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\U
0x000000007ec8c4f0	3	1	R--rd	Device\HarddiskVolume1\ProgramData\Microsoft\Diagnosis\Sideload
0x000000007ec8cc48	1	1	RW----	Device\HarddiskVolume1\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
0x000000007ec8d498	1	0	R--r--	Device\HarddiskVolume1\Users\IEUser\AppData\LocalLow\Microsoft\Cryptnet\UrlCache\MetaData\CC197
0x000000007ec8d5f8	7	0	R--r--	Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Caches\{AFE017C6-E4FE-42FD-90D6-99AED7E8B}

File berhasil dicache oleh memory. Saatnya untuk mengekstrak filenya.

Mengekstrak file berdasarkan process yang menarik

File .snt ini dapat diekstrak dengan modul dumpfiles dari volatility.

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 dumpfiles -Q 0x000000007ec88ce0 -n -D <output directory>
```



Parameter -Q digunakan untuk mempercepat proses pencarian file. Alih-alih menggunakan cara cepat ini, ada juga cara lain mengekstrak dengan cara mengekstrak seluruh file yang berekstensi .snt pada dump dengan cara:

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 dumpfiles -r snt$ -i -n -D <output directory>
```

Outputnya adalah sebuah file yang berhasil diekstrak.

Mendapatkan flagnya

Apabila cara di atas digunakan, seharusnya file yang terekstrak adalah satu dari dua file ini:

 file.1968.0x864870b8.dat	1/18/2021 4:50 PM	DAT File	4 KB
 file.None.0x864870b8.StickyNotes.snt.dat	1/18/2021 6:35 PM	DAT File	4 KB

Kemudian buka file tersebut dengan text editor apapun, terdapat flag yang diobfuscate dengan ROT13.

Input	length: lines:
nen2021{v_fhccbfr_fgvp1_abgrf_jnf_znqr_sbe_vasbezngvba_gb_fgvp1_nebhaq}	

Output	time length lines
ara2021{i_suppose_sticky_notes_was_made_for_information_to_stick_around}	

FLAG:

ara2021{i suppose sticky notes was made for information to stick around}

Cara alternatif yang naif

Menggunakan `strings` akan sangat verbose dan memakan waktu lama. Namun ada beberapa aplikasi yang cukup cepat dalam menemukan flagnya secara naif.

Aplikasi: Hex Editor (HxD)

Kata kunci pencarian: `2021` dengan Little-Endian Encoding

Hasil:

377E8C0	77 00 20 00 74 00 6F 00 20 00 72 00 6F 00 74 00	w. .t.o. .r.o.t.
377E8D0	61 00 74 00 65 00 20 00 74 00 65 00 78 00 74 00	a.t.e. .t.e.x.t.
377E8E0	20 00 69 00 6E 00 20 00 6D 00 73 00 20 00 70 00	.i.n. .m.s. .p.
377E8F0	61 00 69 00 6E 00 74 00 0D 00 0A 00 6E 00 65 00	a.i.n.t....n.e.
377E900	6E 00 32 00 30 00 32 00 31 00 7B 00 76 00 5F 00	n.2.0.2.1.{.v._.
377E910	66 00 68 00 63 00 63 00 62 00 66 00 72 00 5F 00	f.h.c.c.b.f.r._.
377E920	66 00 67 00 76 00 70 00 78 00 6C 00 5F 00 61 00	f.g.v.p.x.l._a.
377E930	62 00 67 00 72 00 66 00 5F 00 6A 00 6E 00 66 00	b.g.r.f._j.n.f.
377E940	5F 00 7A 00 6E 00 71 00 72 00 5F 00 73 00 62 00	_z.n.q.r._s.b.
377E950	65 00 5F 00 76 00 61 00 73 00 62 00 65 00 7A 00	e._v.a.s.b.e.z.
377E960	6E 00 67 00 76 00 62 00 61 00 5F 00 67 00 62 00	n.g.v.b.a._g.b.
377E970	5F 00 66 00 67 00 76 00 70 00 78 00 5F 00 6E 00	_f.g.v.p.x._n.
377E980	65 00 62 00 68 00 61 00 71 00 7D 00 0D 00 0A 00	e.b.h.a.q.)....
377E990	0D 00 0A 00 49 00 4D 00 50 00 4F 00 52 00 54 00	...I.M.P.O.R.T.
377E9A0	41 00 4E 00 54 00 0D 00 0A 00 74 00 68 00 69 00	A.N.T.....t.h.i.
377E9B0	73 00 20 00 69 00 73 00 20 00 61 00 20 00 76 00	s. .i.s. .a. .v.
377E9C0	65 00 72 00 79 00 20 00 69 00 6D 00 70 00 6F 00	e.r.y. .i.m.p.o.
377E9D0	72 00 74 00 61 00 6E 00 74 00 20 00 6D 00 65 00	r.t.a.n.t. .m.e.
377E9E0	73 00 73 00 61 00 67 00 65 00 0D 00 0A 00 74 00	s.s.a.g.e.....t.
377E9F0	68 00 65 00 20 00 74 00 72 00 75 00 74 00 68 00	h.e. .t.r.u.t.h.
377EA00	20 00 69 00 73 00 0D 00 0A 00 74 00 68 00 69 00	.i.s.....t.h.i.
377EA10	73 00 20 00 69 00 73 00 20 00 61 00 20 00 68 00	s. .i.s. .a. .h.
377EA20	79 00 70 00 65 00 72 00 2D 00 76 00 0D 00 0A 00	y.p.e.r.-v....
377EA30	3A 00 28 00 0D 00 0A 00 0D 00 0A 00 00 00 00 00	:(.....
377EA40	D8 11 F2 26 E3 60 00 00 38 66 2A 00 08 4D 2A 00	0.0&ã`..8f*..M*.

Checksum Search (346 hits)

Offset	Excerpt (hex)	Excerpt (text)
82CD706	2F 00 6F 00 74 00 68 00 65 00 72 00 73 00 2F 00 32 00 30 00 32 00 31 00 2F 00 30 00 31 00 2F 00	/.o.t.h.e.r.s./2.0.2.1/.0.1./.
85920CC	3A 00 32 00 08 00 00 00 90 90 51 01 D0 FF FF FF 32 00 30 00 32 00 31 00 2F 00 30 00 31 00 2F 00	::2.....Q.ÿÿÿÿ2.0.2.1/.0.1./.
85921D4	61 6E 6E 65 64 61 63 68 61 67 65 5F D0 FF FF FF 32 00 30 00 32 00 31 00 2F 00 30 00 31 00 2F 00	annedackage_ÿÿÿÿ2.0.2.1/.0.1./.
86B5456	61 00 69 00 6E 00 74 00 0D 00 6E 00 65 00 6E 00 32 00 30 00 32 00 31 00 7B 00 76 00 5F 00 66 00	a.i.n.t....n.e.n.2.0.2.1{.v._f.
877E902	69 00 6E 00 74 00 0D 00 0A 00 6E 00 65 00 6E 00 32 00 30 00 32 00 31 00 7B 00 76 00 5F 00 66 00	i.n.t.....n.e.n.2.0.2.1{.v._f.
880D6D2	50 00 65 00 72 00 73 00 69 00 73 00 74 00 5F 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 38 00	P.e.r.s.i.s.t._2.0.2.1.0.1.1.8.
8837EDC	00 00 49 00 45 00 57 00 49 00 4E 00 37 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 38 00	..I.E.W.I.N.7--2.0.2.1.0.1.1.8.
89BD6D4	73 6F 6C 76 65 64 74 65 6F 73 6F 66 D0 FF FF FF 32 00 30 00 32 00 31 00 2D 00 30 00 31 00 2D 00	solvedteosofÿÿÿÿ2.0.2.1--.0.1--.
8B6E53A	70 00 31 00 5F 00 67 00 64 00 72 00 2E 00 31 00 32 00 30 00 32 00 31 00 30 00 2D 00 31 00 35 00	p.1._g.d.r...1.2.0.2.1.0--1.5.
907D8RF	72 65 66 69 78 00 00 00 00 D0 FF FF FF 3A 00 32 00 30 00 32 00 31 00 30 00 31 00 30 00 34 00	refix.....Dÿÿÿÿ2.0.2.1.0.1.0.4.

Cara alternatif yang tidak naif namun lebih sulit

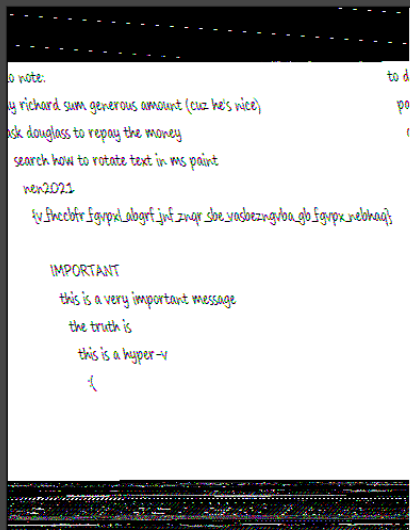
Semua proses yang memiliki UI, pasti UI tersebut juga ditaruh di memory. Dengan melakukan dump memory untuk proses tersebut, kita bisa melihat isi sticky notes tersebut tanpa melihat isi filenya.

PID dari Sticky Notes adalah 1968.

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 memdump -p 1968 -D <lokasi directory output>
```

Akan ada keluaran file 1968.dmp pada directory output. Buka file tersebut di GIMP dengan cara membuka GIMP > File > Open... kemudian centang Show All Files dan pada menu Select File Types, pilih Raw Image Data.

Dengan scrolling parameter dan intuisi proses gambar, flag akan terlihat bersamaan dengan data sticky notes lainnya.



Image

Image Type: RGB

Offset: 191864912

Width: 377

Height: 528

Palette

Palette Type: R, G, B (normal)

Offset: 0

Palette File: (None)

Help

Open

Cancel